National Aeronautics and
Space Administration

John C. Stennis Space Center
Stennis Space Center, MS
39529-6000

SPD 2810.1 Rev. A
October 2004

COMPLIANCE IS MANDATORY

John C. Stennis Space Center
Policy Directive
Information Technology (IT) Network Security

Stennis Policy Directive	SPD 2810.1 *Number*	A *Rev.*
	Effective Date: October 25, 2004	
	Expiration Date: September 3, 2009	
		Page i of ii
Responsible Office: Center Operations Directorate **SUBJECT: Information Technology (IT) Network Security**		

Document History Log

Status/Change/ Revision	**Change Date**	**Originator/Phone**	**Description**
Basic	September 2004	SSC IT Security Manager, James Cluff (228) 688-2249	Initial Release
Rev. A	October 2004	Renay Nelson	Revalidated per NASA Rules Review

Table of Contents

Stennis Policy Directive	SPD 2810.1	A
	Number	*Rev.*
	Effective Date: October 25, 2004	
	Expiration Date: September 3, 2009	
	Page 1 of 24	
Responsible Office: Center Operations Directorate **SUBJECT: Information Technology (IT) Network Security**		

1. POLICY

a. John C. Stennis Space Center (SSC) will develop and implement a comprehensive, but cost effective program for ensuring the security of Information Technology (IT) throughout its life cycle in accordance with federal, regulatory, and NASA requirements.

b. Information Technology security encompasses the planning, acquiring, managing, controlling, and using SSC IT network resources to accomplish National Aeronautics and Space Administration (NASA) and SSC's missions and programs efficiently, effectively, and securely.

c. The policy or policies stated herein conform to and are intended to supplement and enhance requirements for effective IT network security program management established by Federal and Agency regulations, NASA Technical Standards (STD's), Policy Directives (NPD's), Procedural Requirements (NPR's), and other statements of IT policy and standards. Where any portion of this document, its attachments, or appendices conflict with NASA or other federal policy, the higher policy will hold.

d. IT network resources are defined as resources located at SSC and directly connected to a NASA managed network. The definition applies to all computers, wireless devices, Personal Digital Assistants (PDA's), routers, firewalls, switches, hubs, repeaters, gateways, and peripherals. Network resources encompass the data and information, computers, ancillary equipment, software, firmware and similar products; facilities that house such resources; operations, services; and related resources used for the acquisition, storage, manipulation, management, movement, control display, switching, interchange, transmission, or reception of data. Acronyms applicable to SSC IT operations, resources, and security are provided in Attachment 1 of this document.

e. SSC IT network resources will be provided and managed consistent with acceptable risks, cost, and performance, as determined by SSC management to ensure that the resources are:

(1) Operated effectively and efficiently producing accurate data and information.

(2) Protected from unauthorized access, alteration, disclosure, destruction, loss, or misuse in operations and processing, storage and/or transmittal.

(3) Available to support critical SSC programs and functions.

(4) Incorporated with general management and hardware and software application controls sufficient to provide cost-effective acquisition, operation, and assurance of accuracy, integrity, and security.

(5) Provided with appropriate technical, personnel, administrative, environmental, and access safeguards before and after operational use.

(6) Operated in compliance with Agency and SSC policies and guidelines.

(7) Operated in compliance with all software licensing conditions (as detailed by the registration/licensing agreements).

(8) Provided with effective measures to ensure that software put to use is free of errors and viruses.

e. Individual policies for specific functional or subject areas are defined and provided as appendixes to this basic policy document. Appendixes may be added as the need for additional subjects and policies are determined and developed. They may also be removed as dictated by requirements.

f. Specific IT standards, procedures, and work instructions to implement NASA and SSC IT policies and perform necessary operations may be issued in subsequent companion and/or supplemental instructions.

g This SPD and its appendixes will remain in effect until revised or rescinded. The document will be reviewed for continuation upon the normal expiration date of this SPD. Appended policies may be reviewed periodically for determination of continued need and appropriateness of content.

2. APPLICABILITY

The policy or policies defined herein apply to all NASA/SSC employees, NASA/SSC contractors, and to the extent appropriate Resident Agency organizations, in achieving NASA/SSC and Agency missions, programs, projects, and institutional requirements. Specifically, the policies prescribed within this document apply to all offices under the management of the SSC Center Director. Other co-located offices are encouraged to adopt these policies to ensure compatibility with systems and processes.

3. AUTHORITY

a. 5 U.S.C. 552, et. seq., the Freedom of Information Act, as implemented by 14 CFR 1201.

b. 5 U.S.C. 552a, the Privacy Act of 1974, P.L. 93-579, as amended.

c. 18 U.S.C. 799, et. seq., Violation of regulations of National Aeronautics and Space Administration.

d. 18 U.S.C. 2510, et. seq., the Electronic Communications Privacy Act, as amended.

e. 40 U.S.C. 759 note, the Computer Security Act of 1987, P L. 100-235, as amended.

f. 40 U.S.C. 140, et. seq., Section 808 of Public Law 104-208, the Clinger-Cohen Act of 1996 [renaming, in pertinent part, the Information Technology Management Reform Act (ITMRA), Division E of Public Law 104-106].

g. 42 U.S.C. 2451, et. seq., the National Aeronautics and Space Act of 1958, as amended.

h. 44 U.S.C. 2510, et. seq., the Paperwork Reduction Act of 1995, P.L. 104-13, as amended.

i. 50 U.S.C. 2401-2420, the Export Administration Act of 1979, as amended, as implemented by the Export Administration Regulations, 15 CFR Part 730-774.

j. Executive Order No. 12958, Classified National Security Information of May 18, 1995.

k. Executive Order No. 13011, Federal Information Technology of July 16, 1996.

l. OMB Circular A-130, Management of Federal Information Resources, Appendix III.

m. NPD 2800.1, Managing Information Technology.

n. NPD 2810.1, NASA Information Security.

Note: The above listed authorities are generally applicable to all IT network activities. The list is not necessarily all-inclusive; additional authorities, executive orders, notices, and directives may apply. In the case where other authorities are indicated, they will be noted within the specific appended subject policy.

4. REFERENCES

All references described here and in the appendices of this document are assumed to be the latest unless otherwise specified.

a. NPD 1382.17, Privacy Act – Internal NASA Direction in Furtherance of NASA Regulations.

b. NPD 1440.6, NASA Records Management.

c. NPR 1441.1, NASA Records Retention Schedules.

d. NPD 1600.2, NASA Security Policy.

e. NPR 1620.1, Security Procedural Requirements.

f. NPR 2810.1, Security of Information Technology.

g. NPR 2800.1, Managing Information Technology.

h. NASA-STD-2813, Firewall Strategy, Architecture, Standards, and Products.

i. NPD 9800.1, NASA Office of Inspector General Programs.

j. CIO Directive 02-95, March 14, 1995, Internet Usage Policy.

k. CIO Executive Notice 01-96, February 20, 1996, NASA Electronic Mail.

l. SPD 2800.2, SSC Information Technology Resources Usage Policy.

Note: The above listed references are applicable to the establishment and management of the SSC IT Network Security Program. This list is not necessarily all-inclusive. Where appropriate and applicable, other specific references may be called out in the appended policies and associated IT instructional publications.

5. RESPONSIBILITY

a. Center Director. The SSC Center Director has oversight responsibilities for ensuring that an effective program for the management of IT is established and maintained for SSC. The Director ensures compliance with Government and NASA IT Directives and appoints a:

(1) Center Chief Information Officer (CIO) to represent the Center on IT matters and coordinate with the NASA CIO to ensure the most effective and efficient oversight of implementation activities to support IT policies, architectures, standards, procedures, practices, initiatives, and services.

(2) Center IT Security Manager (ITSM) who provides organization and direction for implementing Center IT Security in coordination with the CIO.

(3) Designated Approval Authority (DAA) for accrediting information resources for processing national security information.

b. Center Chief Information Officer. The SSC CIO is responsible for establishing an effective and economical IT Program at SSC as defined in NASA directives NPD 2800.1 and NPR 2800.1, Managing Information Technology and NPD 2810.1, NASA Information Security. The CIO responsibilities include but are not limited to:

(1) Establishing, implementing, and maintaining computer architectures, standards, best practices, policies, and guidance to assure the secure operation of SSC Systems and the protection of the SSC’s data and information.

(2) Ensuring that sufficient resources are budgeted and available to implement and maintain the technical and security controls of the SSC's IT infrastructure.

(3) Assuring that the computer infrastructure has built-in recovery features (availability), provides adequate baseline protections (confidentiality), and protects data from modifications (integrity).

(4) Reviewing the SSC IT network for alignment and compliance with Federal, NASA and SSC IT regulatory requirements, and directions.

(5) Coordinating and approving SSC’s responses to required IT plans, budgets, reports, and audits.

(6) Participating in SSC’s reengineering and continuous improvement processes by advocating the appropriate utilization of the IT network.

(7) Obtaining and reviewing metrics from SSC organizations relating to IT network planning, investment, returns, and appropriate utilization.

(8) Ensuring the protection of all information (physical and electronic) and the SSC IT network resources and enforcing NASA information security policies and procedures and Federal information security policy.

c. Directors, Program Managers, and Office Heads. The Directors of SSC Directorates, Managers, and office heads are responsible for:

(1) Planning, budgeting, and funding the acquisition, management, and use of IT resources under their direct management control and ensuring the incorporation of IT security into the life cycle.

(2) Preparing data for integration into required SSC IT plans, reports, and audits.

(3) Assuring compliance with Federal regulations, NASA directives, and SSC's IT network security program.

(4) Appropriate screening, approval, and training of personnel for the access and use of SSC IT resources.

d. IT Security Manager. The ITSM is responsible for the overall management of the SSC IT Security Program and specifically for the following:

(1) Coordinating IT security activities with the CIO and developing and issuing directives necessary to implement the SSC IT Security Program.

(2) Developing, implementing, and monitoring the SSC IT Security Plan.

(3) Supporting and coordinating with the Training Office to develop a SSC IT Security Awareness and Training Plan for implementing a training program that adheres to Agency initiatives and direction for IT security awareness and training.

(4) Establishing a process to ensure that appropriate screening has been completed for individuals requesting system privileges.

(5) Conducting periodic reviews and compliance checks to ensure: [1] SSC IT Security Plans are current or a plan for updating is in place, [2] Significant changes to hardware, software, or operating environments are analyzed and documented for risk impact, and [3] SSC IT security policies and guidelines are current and comply with Federal and NASA regulations.

(6) Maintaining documentation on SSC IT Security Plans, significant IT security incidents, audits, and evaluations; and establishing procedures for reporting metrics to management.

(7) Coordinating with the Center Chief of Security (CCS), Local Office of Inspector General (OIG), and the SSC IT Security Incident Response Team (IRT) to gather intelligence data regarding threats, concerns, and hacker techniques affecting the vulnerability of NASA information and systems.

(8) Responding appropriately to SSC IT security incidents by: [1] Organizing and directing inquiries, examinations, and corrective actions, [2] Establishing and maintaining a technically oriented IT IRT, [3] Reporting incidents to SSC and Agency management and to the OIG, as necessary, and [4] Conducting penetration testing to ensure that controls are effective.

e. Designated Approval Authority. The DAA is responsible for accrediting SSC information resources that process national security information (i.e., classified information). By accrediting a system, the DAA formally assumes responsibility for the operation of the system within a specified environment.

f. Telecommunications Manager. The SSC Telecommunications Manager is responsible for administering and managing SSC telecommunications functions encompassing infrastructure, voice and voice/data, facsimile, office automation desktop services, network connectivity, and radio and paging services. The Telecommunications Manager responsibilities include but are not limited to:

(1) Coordinating telecommunications activities with the CIO and developing and issuing directives necessary to implement telecommunications requirements.

(2) Planning, budgeting, funding, and approving the acquisition, management, and use of telecommunications resources and services.

(3) Ensuring telecommunications compliance with Federal regulations and NASA/SSC requirements and directions.

g. System Computer Security Officials. System Computer Security Officials (CSO's), designated by management, are responsible for the SSC IT Security Program for their systems. They serve as the critical communication link to and from their organizations for all IT security matters. Their responsibilities for IT are as follows:

(1) Establishing management controls and a communications process to ensure that SSC’s implementation of the IT program and its security is consistent with mission needs and NASA policies and guidance.

(2) Serving as SSC’s representative to the ITSM and representing the SSC Line Managers on security matters.

(3) Reporting periodically to the ITSM and the organization’s senior manager on the status of the SSC IT security posture.

(4) Ensuring the preparation and annual review of SSC IT Security Plans for their Systems.

h. Center Line Managers. SSC Line Managers (LMs) are responsible for IT security for their systems. Their responsibilities for IT security are as follows:

(1) Ensure that the security risks of SSC systems under their cognizance are identified and evaluated and that adequate safeguards are implemented.

(2) Certify the adequacy and appropriateness of security controls before putting any new systems into operation. Periodically conduct the same certification throughout the life cycle of the system.

(3) Ensure that a properly trained System Administrator (SA) is assigned as the focal point for the security of each system or application.

i. Center Chief of Security. The SSC CCS is responsible for providing oversight, guidance, and approval authority for projects conducting classified activities. The CCS conducts appropriate personnel security screening for those working in sensitive positions and those who can bypass IT technical security controls and processes. The CCS coordinates, investigates, and approves requests for foreign nationals who require access to systems, applications, and networks operated by or on behalf of NASA. In conjunction with the CIO and/or ITSM, the CCS is also responsible for the coordination of investigations of information security incidents and computer crimes.

j. Center Training Office. The SSC Training Office is responsible for coordinating with the ITSM to develop a SSC IT Security Awareness and Training Plan.

k. Center Acquisition Management Office. The SSC Acquisition Management Office is responsible for assuring that IT network acquisitions are approved and that appropriate security requirements are included in existing contracts, specifications and/or statements of work for IT Security acquisitions or operations of IT installations, equipment, software, and related services. The Procurement office, working with the SSC CIO and the SSC ITSM, is responsible for:

(1) Identifying acquisitions for computer hardware, software, data management, and support services.

(2) Establishing a joint process with the SSC CIO and ITSM to review acquisitions of SSC IT network resources.

(3) Ensuring that all procurement actions, including solicitations and contracts, comply properly with IT network and IT security policies, procedures, and guidance.

l. SSC IT Network Manager. The SSC NASA IT Network Manager (ITNM) is responsible for the architectural, engineering, and security aspects of the SSC network. The ITNM is responsible for:

(1) Enforcing and monitoring compliance with the network security policy.

(2) Providing direction to the NASA Network Control Contractor (NNCC) in the management of the SSC network.

(3) Monitoring network traffic at SSC and investigating possible inappropriate traffic or connections.

(4) Serving as a member of the SSCLAN Configuration Control Board (CCB).

(5) Serving as a member of the SSCLAN Firewall CCB.

m. SSCLAN Configuration Control Board. The SSCLAN CCB provides overall policies for network design and architecture.

n. SSCLAN Firewall Configuration Control Board. The Firewall CCB is responsible for overseeing the firewall rules that define ports and services into SSC.

o. NASA/SSC Contractors. SSC Contractors are responsible for:

(1) Establishing the necessary management controls and a communications process to ensure that implementation and performance of the IT network activities is in accordance with requirements and all NASA/SSC policies and guidance.

(2) Appropriate screening, approval, and training of personnel for the access and use of SSC IT resources.

(3) Complying with SSC NASA IT security policies and procedures, and reporting IT security incidents or unauthorized access to the NASA IT Security Office.

p. SSC Employees and Visitors. Employees and visitors will comply with SSC NASA IT security policies and procedures, and report IT security incidents or unauthorized access to the NASA IT Security Office.

6. CANCELLATION

SPD 2810.1 Basic

Signature on file

T. Q. Donaldson V, RDML USN (Ret)
Director

ATTACHMENTS

DISTRIBUTION

Approved for public release via NODIS; distribution is unlimited.

ATTACHMENT 1 - ACRONYMS

AIS	Automated Information Systems (also see IT – Information Technology)
AOL	America On Line (Internet Service Provider)
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AT&T	American Telephone and Telegraph
BRT	Business and Restricted Technology
CCB	Configuration Control Board
CCS	Center Chief of Security
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CSO	Chief Security Officer
DAA	Designated Approval Authority
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Naming System
ELAN	Emulated Local Area Network
E-Mail	Electronic Mail
GRE	General Routing Encapsulation
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IG	Inspector General
IPSEC	Secure Internet Protocol
IRC	Internet Relay Chat
IRT	Incident Response Team
ISP	Internet Service Provider
IT	Information Technology
ITNM	Information Technology Network Manager
ITMRA	Information Technology Management Reform Act

ITSM	Information Technology Security Manager
INS	Integrated Network Services
LAN	Local Area Network
LM	Line Manager
MAC	Media Access Control
MSN	Mission Critical
NASA	National Aeronautics and Space Administration
NFS	Network File System/Server
NISSU	NASA Information Systems Services Utility
NNCC	NASA Network Control Contractor
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements (formerly NPG, NASA Procedures and Guidelines
NSA	National Security Agency
ODIN	Outsourcing Desktop Initiative for NASA
OIG	Office of Inspector General
OMB	Office of Management and Budget
PC	Personal Computer
PDA	Personal Digital Assistant
POC	Point of Contact
PPTP	Point-To-Point Tunneling Protocol
RAM	Random Access Memory
RAS	Remote Access System
ROM	Read-Only Memory
SA	System Administrator
SPD	Stennis Policy Directive
SSC	Stennis Space Center
STD	Technical Standard
STS	Stennis Technical Standards

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX A: 2810.1(1) – GENERAL NETWORK CONTROLS

A.1.0 PURPOSE AND OBJECTIVE

All IT resources at SSC, such as data, information, applications, and systems, are considered to be valuable and sensitive to some degree. This policy covers network and computer security for all devices connected to SSC NASA managed networks (SSCLAN's), in order to protect SSC IT resources from threats and attacks originating primarily from outside the SSC environment.

This policy establishes the general network controls that will be used by the Stennis Space Center (SSC) to ensure that the safeguards for the protection of the integrity, availability, and the confidentiality of IT resources are fully integrated into and support the mission of NASA and SSC.

A.2.0 POLICY

a. SSC will comply with prescribing NASA and Federal regulations on IT security to ensure adequate protective measures, risk assessments, and IT security plans are in place for all IT resources.

b. Any system or service that poses an unacceptable risk as determined by SSC IT Security Manager (ITSM) or designee or the SSCLAN Configuration Control Board (CCB) to any other SSC system or service on a SSCLAN will be disconnected. Violations may be subject to review by SSC Management, the NASA Inspector General (IG), or other law-enforcement agencies.

c. All devices that connect to a SSCLAN network must register the Media Access Control (MAC) address via the SSC NASA Network Control Contractor (NNCC) for a NASA controlled static IP address. The minimum information required for network registration is system tag number, system point of contact (POC) with telephone number, location (building and room number), network jack number, MAC address, and system name. Any unregistered systems or systems detected using an un-authorized IP address shall be disconnected from the SSC network until an investigation is completed, a correction applied, and management notification made as to the security impacts/risks encountered. The use of Dynamic Host Configuration Protocol (DHCP) is strictly prohibited unless an explicit waiver is obtained from the ITSM or the SSC IT Network Manager (ITNM).

d. All IT resources connected to SSCLAN will meet the minimal IT security standards as defined by the ITSM to include, but not limited to:

(1) Display of the government Warning Banner.

(2) Expeditious installation of IT security patches.

(3) Restriction of access to the resources to the greatest extent possible, to include the use of IP wrapper software.

(4) Restriction of unnecessary file sharing to the greatest extent possible.

(5) Disabling of network services/ports that are not utilized from automatic start-up.

(6) Performance of regular, periodic back-ups and verification of restorability.

(7) Compliance with the use of strong passwords.

(8) Periodic review of system logs (weekly at a minimum) for unauthorized access.

(9) Maintenance of current anti-virus software that is configured for the automatic downloading of the latest virus definition files and scanning of all files when they are opened.

e. Systems connected to the SSCLAN cannot be added to or moved unless their civil servant line management has prior permission and the move is coordinated with the NNCC. Line Managers (LM's) must certify to the Computer Security Officers (CSO's) that the system meets the minimum criteria as outlined in the Network Configuration document. Systems found not to be in compliance with minimal criteria, shall be disconnected from the network until corrective action is applied.

f. Network scanning is restricted to the SSC IT Security Team. With approval from their CSO and coordination with the SSC IT Security Team, system administrators can conduct scanning of their organizational networks.

g. The use of network/computer attack tools and network/system discovery tools and network/system monitoring tools is strictly prohibited unless an explicit waiver is obtained from the ITSM or the ITNM. Systems found to be running these tools shall be disconnected from the network until the ITSM and the ITNM complete a review.

h. All networking devices, i.e., hubs, switches, routers, etc., will be placed in authorized locations such as communication closets or other areas approved by the SSCLAN CCB. Only the SSCLAN CCB may grant an exception to this policy. Networking devices located in unauthorized locations shall be disconnected from the network and confiscated by the ITSM or ITNM.

i. All network wiring installed and utilized on the SSCLAN shall be in compliance with SSC wiring standards as outlined in the SSC Network Wiring Standards (STS-2810-0001).

j. All analog telephone lines must be approved by the ITSM.

k. The use of a modem is not allowed on any system connected to the SSCLAN unless registered with and an explicit waiver obtained from the SSCLAN CCB or the ITSM.

l. Any type of remote access (dial-in, Virtual Private Network [VPN], etc.) must be approved by the SSCLAN CCB or the ITSM.

m. The sharing of computer resources with external (off-center) computer projects (PC philanthropy) is not allowed.

n. Peer-to-peer networking processes with external (off-center) computers or networks (examples - Microsoft sharing and printing, UNIX NFS, AppleTalk Shares, Bearshare, Limewire, etc.) are not allowed.

o. The use of Internet Relay Chat (IRC) programs with external (off-center) computers or networks (examples - Instant Messages such as AOL, Yahoo, and MSN, Chat Rooms, etc.) is not allowed.

p. The use of e-mail (read/send messages) on a system connected to the SSCLAN from any external (off-center) provider (Yahoo, AOL, Hot-mail, AT&T, Lotus Notes, etc.) is not allowed.

q. The use of network control applications (Timbuktu, PC Anywhere, NetMeeting, WebExpress, etc.) that allow control of local SSC systems across the external SSC boundaries is strictly prohibited unless registered with or an explicit waiver obtained from the SSCLAN CCB or the ITSM. Systems found to be running these tools shall be disconnected from the network until a review is completed by the ITSM and ITNM.

r. The use of network IP tunnels (IPSEC, PPTP, GRE, HTTP, etc.) of local SSC systems across the External SSC boundaries are strictly prohibited unless registered with or an explicit waiver obtained from the SSCLAN CCB or the ITSM. IPSEC protocols originating from/to internal networks or computers to external network or computers will undergo IT security and network testing review. Split tunneling when in an IPSEC tunnel is forbidden when tunneling between an on-site SSC computer system or network and off-site system or network. Systems found to be running these tools shall be disconnected from the network until a review is completed by the ITSM and ITNM.

s. Visiting personnel may not connect their computers to the Private or Public LANs. Connections are only allowed on the Open network and must be coordinated with the ITNM. See Network Configuration Policy.

t. The download and installation of freeware, shareware, or any other public domain software and/or commercial software from any foreign site, bulletin board, university, Internet Service Provider (ISP), or any non-commercial site is not allowed.

u. Users must report any computer compromise immediately to the NASA IT Security Office (http://security.ssc.nasa.gov/report.htm).

v. The use of "Intrusion Detection Devices" is not allowed on any system connected to the SSCLAN unless registered with and an explicit waiver obtained from the SSCLAN CCB or the ITSM.

w. The use of a "sniffer" is not allowed on any system connected to the SSCLAN unless registered with and an explicit waiver obtained from the SSCLAN CCB or the ITSM.

A.3.0 APPLICABILITY

The policy or policies defined herein apply to all individuals and IT resources located at SSC and are directly connected to the SSCLAN. This includes civil service, contractor, tenant, and outsource personnel. The policy also applies to all computers, wireless devices, Personal Device Assistants (PDA's), routers, peripherals, and other devices.

A.4.0 AUTHORITIES AND REFERENCES

See Master SSC Network Policy.

A.5.0 RESPONSIBILITY

See Master SSC Network Policy.

A.6.0 CANCELLATION

SPD 2810.1 Basic Appendix A
This policy will remain in effect until revised or rescinded.

APPENDIX B: 2810.1(2) – NETWORK CONFIGURATION

B.1.0 PURPOSE AND OBJECTIVE

All Information Technology (IT) resources at the Stennis Space Center (SSC), such as data, information, applications, and systems, are considered to be valuable and sensitive to some degree. This policy covers network and computer security for all devices connected to SSC NASA/Outsourcing Desktop Initiative for NASA (ODIN) managed networks (SSCLAN's), in order to protect SSC IT resources from threats and attacks originating primarily from outside the SSC environment.

B.2.0 POLICY

The SSCLAN will have three (3) separate (private, public, and open) Local Area Networks (LAN's), with different levels of access security. Each network will be protected by a combination of firewalls, intrusion detection, and host level security. In addition, a Border Router will further insulate all three (3) networks from the Internet. The SSCLAN Configuration Control Board (CCB) provides overall policies for network design and architecture. The Firewall CCB is responsible for overseeing the firewall rules that define ports and services into and out of SSC. The Firewall CCB works in conjunction with the SSCLAN CCB and organizational Computer Security Officers (CSO's) to review and approve changes to the network.

a. Private Network. The Private Network contains SSC's critical resources (such as mission-critical systems, restricted group servers, non-public servers, and end-user computer systems) that require strong security protection from the Internet. The Private Network contains multiple sub-networks (containers) separated by an additional level of protection using firewalls and/or access control lists. Examples of Private Networks are agency/function/program networks, Center-specific resources, and Extranet.

(1) External access (i.e. connections from remote dialup or networks) is restricted to SSC Chief Information Officer (CIO) approved access methods that employ strong user authentication and/or encryption.

(2) All accounts for external access into the Private Network must be approved in writing by civil servant line management.

(3) Dial-up into the Private Network is restricted to the central SSC Remote Access System (RAS), the central SSC Virtual Private Network Gateway (VPN) and other Center approved gateways that reside outside the Private Network.

(4) Computers on the Private Network are prohibited from using modems, computer faxes, T-1 Lines, and similar links unless registered with and an explicit waiver obtained from the ITSM. This would create a bridge between the Private Network and an outside network.

(5) Multi-homed connections (computers with multiple network cards) are prohibited from directly connecting (bridging) to networks outside the Private Network.

(6) Computers that require direct access by the public are prohibited.

(7) Visiting personnel may not connect their computers to the Private Network.

b. Public Network. The Public Network is intended for highly visible information servers that must be accessible by the public or collaborators, but requires very substantial protection to assure uncompromised information integrity and service availability. This includes Public Web Servers, File Servers, E-mail servers, Directory Services, and various Collaborative Services. Networks that fit the Public Network description include the Demilitarized Zone (DMZ) and Campus Network.

(1) Access rules, for servers on the Public Network, must be developed by the system administrator (SA), line manager (LM), and CSO and approved by the IT Security Manager (ITSM) and IT Network Manager (ITNM).

(2) Remote system administration must be done using CIO-approved secure methods. Where this is not possible, the system must be administered from its console.

(3) Systems on the Public Network must be dedicated as servers (with exceptions for security, network, and backup services, and local peripheral systems).

(4) User workstations are not permitted on the Public Network.

(5) Public Network servers may not serve in a dual capacity as a user workstation.

(6) Systems that do not require public access are not permitted on the Public Network.

(7) Systems on the Public Network are prohibited from using modems, computer faxes, T-1 lines, and similar links.

(8) Multi-homed connections (computers with multiple network cards) are prohibited from directly connecting (bridging) to networks outside the Public Network links unless registered with and an explicit waiver obtained from the SSCLAN CCB.

(9) Systems are not permitted to originate connections into the Private Network without using strong authentication and encryption and must have NASA SSCLAN CCB approval.

(10) Visiting personnel may not connect their computers to the Public Network.

c. Open Network. The Open Network, also known as the Victim Network or Guest Network, contains computer resources that need to be freely accessible by the scientific community of the public-at-large and cannot function under the security rules of the Private and Public Networks. These resources require protection in terms of data integrity and availability, rather than extensive security measures that might hamper collaboration of other communications.

(1) The Open Network has limited security and is considered untrusted.

(2) Modems, T-1 lines, computer faxes, and other similar connections are permitted on the Open Network.

(3) Multi-homed connections from the Open Network to the other external networks are permitted, but are not allowed to the Private and Public Networks.

(4) Access from the Open Network to the Private Network is treated as an external, untrusted connection and requires user authentication and encryption.

(5) Systems are permitted on the Open Network upon the written approval of the NASA LM that certifies to the CSO that the risks are accepted and approved by the ITSM.

(6) Connectivity to this network is subject to the SSCLAN CCB review.

(7) Mission Critical (MSN) and Business and Restricted Technology (BRT) systems are not allowed on the Open Network.

B.3.0 APPLICABILITY

The policy or policies defined herein apply to all individuals and IT resources located at SSC and are directly connected to the SSCLAN. This includes civil service, contractor, tenant, and outsource personnel. The document also applies to all computers, wireless devices, Personal Device Assistants (PDA's), routers, peripherals, and other devices.

B.4.0 AUTHORITIES AND REFERENCES

See Master SSC Network Policy.

B.5.0 RESPONSIBILITY

See Master SSC Network Policy.

B.6.0 CANCELLATION

SPD 2810.1 Basic Appendix B
This policy will remain in effect until revised or rescinded.

APPENDIX C: 2810.1(3) – NETWORK MANAGEMENT

C.1.0 PURPOSE AND OBJECTIVE

All Information Technology (IT) resources at the Stennis Space Center (SSC), such as data, information, applications, and systems, are considered to be valuable and sensitive to some degree. This policy covers network and computer security for all devices connected to SSC NASA/Outsourcing Desktop Initiative for NASA managed networks (SSCLAN's), in order to protect SSC IT resources from threats and attacks originating primarily from outside the SSC environment.

C.2.0 POLICY

The SSCLAN will have three (3) separate (private, public, and open) Local Area Networks (LANs), with different levels of access security. Each network will be protected by a combination of firewalls, intrusion detection, and host level security.

a. The SSCLAN follows the recommended practice for Center protection, as outlined in the Agency recommendation for Firewall Implementation. The first layer is the border router. The NASA Information Systems Services Utility (NISSU) wide area network (WAN) Center router currently provides the border router function. The border router shall follow configuration recommendations as outlined in the National Security Agency (NSA) Router Document. The next layer is the Center Firewall router.

b. The Stennis Firewall is placed in a deny-based posture and follows the Agency recommendation for Firewall Perimeter rule base. Access to the Center is restricted unless specifically allowed. System, applications, processes, or users that require access to other systems, applications, processes, or users must go through a formal review process with the SSCLAN Configuration Control Board (CCB).

c. Individual IP addresses are assigned, controlled, and managed by the NASA Network Control Contractor (NNCC) contractor under direction of the NASA IT Network Manager (ITNM).

d. Address blocks are assigned by the ITNM and approved by the SSCLAN CCB. The blocks of addresses are grouped by program, by agency, or by purpose.

e. The SSCLAN is comprised of an Asynchronous Transfer Mode (ATM) backbone that provides connections to Gigabit, Fast Ethernet, and 10 Megabit connections. SSC has three (3) types of LANs – Emulated Local Area Networks (ELAN's), Virtual Local Area Networks (VLAN's) and conventional LANs. ELAN's, VLAN's, and LAN's are created when the network requirements are identified that would benefit by a unique ELAN, VLAN, or LAN and approved by the ITSM or the Firewall CCB. In order for an ELAN, VLAN, or LAN, to become viable on the SSSCLAN, approval must be obtained from the ITNM or the SSCLAN CCB.

f. All network ports on the SSCLAN are secured by “port locking” (i.e. each network device is known on the network by its unique Media Access Control (MAC) address which is associated with a port on a network infrastructure switch). The exceptions to this policy are as follow:

(1) Conference Rooms. Conference room connections are network jacks located in conference rooms. The network connections are cross-connected or strapped in the network wiring closets but are electronically turned off unless they are associated with a permanently located conference room computer. If a permanent computer is located in the conference room, then the port is locked.

(2) Test Connections. Test connections are normally associated with network devices that “roam” (no permanent location, like notebook or laptop computers). Test connection requests require a waiver from the Network Configuration Control Board.

g. The use of dial-in, Virtual Private Network (VPN), and Citrix access and remote administration of network servers and network devices requires the use of two-factor authentication mechanism. SSC has deployed the use of a hardware token, SecureID.

h. All Network protocols allowed on the SSCLAN must be approved by the SSCLAN CCB and the ITNM. Examples of such are listed but are not limited to UDP, TCP, ICMP, ARP, IPSEC, and AppleTalk. Any non-approved protocols found on the network shall be removed until a waiver is filed with and approved by the SSCLAN CCB.

i. All AppleTalk architecture and implementation of zone names, ranges, and zone information are to be managed by the NNCC and approved by the ITNM. Any changes must be coordinated through the SSCLAN CCB.

j. All Windows architecture and implementations are coordinated through the ITNM and approved by the SSCLAN CCB. The information to be recorded consists of, but not limited to all domain controllers and active directory components.

k. All computer/system/device names shall be registered with the NNCC. Names shall be unique and shall begin with SSC. Primary name shall map to SSCTag# of system. An alias may be established but must be unique.

C.3.0 APPLICABILITY

The policy or policies defined herein apply to all individuals and to the IT resources located at SSC that are directly connected to the SSCLAN. This includes civil service, contractor, tenant, and outsource personnel. The document also applies to all computers, wireless devices, Personal Device Assistants (PDA's), routers, peripherals, and other devices.

C.4.0 AUTHORITIES AND REFERENCES

See Master SSC Network Policy.

C.5.0 RESPONSIBILITY

See Master SSC Network Policy.

C.6.0 CANCELLATION

SPD 2810.1 Basic Appendix C
This policy will remain in effect until revised or rescinded.